IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS

PORSCHA DILLARD, individually and on behalf all others similarly situated, Plaintiff(s), v. ORDER EXPRESS, INC., Defendant.	Case No._____ **CLASS ACTION COMPLAINT** **Demand For Jury Trial**

CLASS ACTION COMPLAINT

Plaintiff(s) Porscha Dillard ("Plaintiff(s)") bring this action, on behalf of themselves and all others similarly situated, against Defendant Order Express, Inc. ("Order Express" or "Defendant"). Plaintiff(s) seek to obtain damages, restitution, and injunctive relief for a class of individuals ("Class" or "Class Members") who are similarly situated and have received notices of the data breach from Order Express. Plaintiff(s) make the following allegations upon information and belief, except as to their own actions, the investigation of their counsel, and the facts that are a matter of public record.

NATURE OF THE ACTION

1. This class action arises out of a 2022 data breach ("Data Breach") of documents and information stored on the computer network of Order Express, a company that offers services including, *inter alia*, money transfer, check cashing, and money orders, loans, and bill payment services.[1]

2. According to its website, Order Express began in Mexico with "its primary activity

[1] *Services*, Order Express, https://www.orderexpress.com.mx/Home/services/ (last visited Dec. 20, 2022).

[being] the fast and secure sending of money."[2]

3. On its computer network, Order Express holds and stores certain highly sensitive personally identifiable information ("PII" or "Private Information") of the Plaintiff(s) and the putative Class Members, who are customers of its various financial services, i.e., individuals who provided their highly sensitive and private information to Order Express in exchange for its business services.

4. According to the Notice of Data Breach Letter that Order Express sent to Plaintiff(s) and Class Members, as well as those it sent to State Attorneys General, it first became aware of the Data Breach on or about September 7, 2022, and began investigating. "The investigation determined an unknown party accessed parts of our computer network without authorization between July 29, 2022 and September 7, 2022."[3]

5. Thus, Order Express did not realize for over a month that the PII of Plaintiff(s) and Class was actively being accessed and exfiltrated by cyber criminals.

6. Order Express finally began notifying the approximately 63,220 victims over 5 months after the Data Breach began, on or about December 15, 2022.

7. As a result of Order Express's Data Breach, Plaintiff(s) and thousands (if not more) of Class Members suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

8. In addition, Plaintiff(s)' and Class Members' sensitive personal information—

---

[2] *About Us*, Order Express, https://www.orderexpress.com.mx/Home/about-us/ (last visited Dec. 20, 2022).

[3] *See Data Breach Notifications–Order Express, Inc.*, Me. Att'y Gen. (Dec. 15, 2022), https://apps.web.maine.gov/online/aeviewer/ME/40/1d501066-b1ca-4bbb-9500-5361bb73b1ac.shtml (last visited Dec. 20, 2022).

which was entrusted to Defendant—is now in the control of cybercriminals, although Defendant claims in the notice letters that "privacy and security of information is important to us, and we will continue to take steps to protect information in our care."[4]

9. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect Plaintiff(s) and Class Members' Private Information.

10. Plaintiff(s) bring this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that they collected and maintained, and for failing to provide timely and adequate notice to Plaintiff(s) and other Class Members that their information had been subject to the unauthorized access of an unknown third party and precisely what specific type of information was accessed.

11. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer network in a condition vulnerable to cyberattacks. The mechanism of the cyberattack and potential for improper disclosure of Plaintiff(s)' and Class Members' Private Information was a known risk to Defendant. Thus, Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

12. Defendant disregarded the privacy and property rights of Plaintiff(s) and Class Members by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that they did not have adequately robust computer systems and security practices to safeguard Class Members' Private Information; failing to take standard and reasonably available

[4] *Id*.

steps to prevent the Data Breach; and failing to provide Plaintiff(s) and Class Members prompt, accurate, and complete notice of the Data Breach.

13. In addition, Defendant and its employees failed to properly monitor the computer network and systems that housed the Private Information. Had Defendant properly monitored its computers, it would have discovered the intrusion sooner, and potentially been able to mitigate the injuries to Plaintiff(s) and the Class.

14. Plaintiff(s)' and Class Members' identities are now at substantial and imminent risk because of Defendant's negligent conduct since the Private Information that Defendant collected and maintained (including Social Security numbers) is now in the hands of data thieves. Plaintiff(s) and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

15. Plaintiff(s) and Class Members may also incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

16. Through this Complaint, Plaintiff(s) seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during the Data Breach (the "Class").

17. Accordingly, Plaintiff(s) bring this action against Defendant for: (i) negligence, (ii) breach of implied contract, (iii) negligence per se, (iv) breach of fiduciary duty; (v) intrusion upon seclusion/ invasion of privacy, (vi) unjust enrichment; and (vii) declaratory judgment. And Plaintiff Dillard brings this action on behalf of herself and a California subclass for: (viii) Violation of the California Unfair Competition Law; (ix) Violation of California Consumers Legal Remedies Act; and (x) Violation of California Consumer Records Act, seeking redress for Order Express's

unlawful conduct.

18. Plaintiff(s) seek remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, statutory damages, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate, long term credit monitoring services funded by Defendant, and declaratory relief.

PARTIES

19. Plaintiff Porscha Dillard is, and at all times relevant to this Complaint was, an individual citizen of the State of California, residing in the city of Riverside (Riverside County). On or about December 19, 2022, Plaintiff Dillard received a Notice of the Data Breach from Order Express. A copy of the notice she received is dated December 15, 2022 like the exemplar Notice Letter[5] attached as Exhibit A (the "Notice Letter").

20. Defendant Order Express, Inc. is an Illinois based for-profit corporation, registered with Illinois pursuant to the Business Corporation Act of 1983, as amended. Order Express's Headquarters are located at 685 West Ohio Street, Chicago, Illinois 60654. Defendant can be served through its registered agent, Isela M. Molina at: 685 West Ohio Street, Chicago, Illinois 60654.

21. All of Plaintiff(s)' claims stated herein are asserted against Defendant Order Express, Inc. and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

JURISDICTION AND VENUE

22. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed

[5] *See Data Breach Notifications–Order Express, Inc.*, Me. Att'y Gen, *supra* note 3.

class, and at least one member of the class is a citizen of a state different from Defendant.

23. The Court has general personal jurisdiction over Defendant because, personally or through its agents, Defendant operates, conducts, engages in, or carries on a business or business venture in Illinois; it is registered with the Secretary of State in Illinois as a Domestic for-profit corporation; it maintains its headquarters in Chicago, Illinois; and committed tortious acts in Illinois.

24. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because it is the district within which Order Express has the most significant contacts.

STATEMENT OF FACTS

Nature of Defendant's Business

25. According to its website, "In 1993, Order Express Inc was born, a proudly Mexican company that is governed by US laws and statutes, determining as its primary activity the fast and secure sending of money."[6] with strong ties to Mexico. Its headquarters is located in Chicago, Illinois, and it has locations in at least 23 states of the United States.[7]

26. Order Express also operates JP Check Cashing Financial and OrderExpress Financial. Upon information and belief, Order Express employed more over 100 people and generated approximately $50 million in annual revenue in 2021.

27. Order Express provides a variety of financial services, including but not limited to: money transfers ("Order Express is one of the most accessible, quickest, and safest solutions in the delivery of funds."); check cashing; loans; domestic and international bill payments; and

[6] *About Us*, Order Express, *supra* note 2.
[7] *Branches*, Order Express, https://www.orderexpress.com.mx/Home/branches/ (last visited Dec. 20, 2022).

international and domestic mail and package delivery.[8]

28. Order Express collects PII of consumers who are seeking its financial and other services. This PII includes, *inter alia,* consumers' full names, dates of birth, multiple forms of contact information including phone numbers, addresses, and email addresses, Social Security numbers, driver's license or other state identification numbers, passport numbers, and other financial and credit information.

29. Order Express, in the regular course of its business, collects and maintains the PII of consumers as a requirement of its business practices.

30. Consumers seeking its services entrusted Order Express with their PII with the mutual understanding that this highly sensitive private information was confidential and would be properly safeguarded from misuse and theft.

31. Order Express promises in it its Privacy Policy that it "endeavor[s] to use reasonable security measures. These measures can include physical, electronic and procedural safeguards such as computer safeguards and secured files and buildings. We also endeavor to limit personal information access to only employees, agents and representatives that need to know."[9]

32. In its Notice Letters, Order Express acknowledges that "privacy and security of information is important to [it], and [it] will continue to take steps to protect information in [its] care."[10]

33. In the course of collecting Private Information from consumers, including Plaintiff(s) and Class Members, Order Express promised to provide confidentiality and adequate

[8] *Services*, Order Express, *supra* note 1.
[9] *Privacy Statement*, Order Express (Feb. 1, 2017), https://www.orderexpress.com.mx/Home/privacy-statement/ (last visited Dec.21, 2022).
[10] *See* Notice Letter, Ex. A.

security for Private Information through its applicable Privacy Policy and in compliance with statutory privacy requirements applicable to the financial services industry.

34. Plaintiff(s) and the Class Members, as consumers, relied on the promises and duties of Order Express to keep their sensitive PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Consumers, in general, demand that businesses that require highly sensitive PII will provide security to safeguard their PII, especially when their Social Security numbers, driver's license, state identification, and passports are involved.

35. In the course of their dealings, Plaintiff(s) and Class Members provided Order Express with all or most of the following types of Private Information:

- First and last names;
- Home addresses;
- Email addresses;
- Phone numbers;
- Social Security numbers;
- Driver's license numbers;
- Passport and visa information;
- Credit history; and
- Bank account or payment card information.[11]

Order Express had a duty to adopt reasonable measures to protect Plaintiff(s)' and Class Members' PII from unauthorized disclosure to third parties.

The Data Breach

[11] *Privacy Statement*, Order Express, *supra* note 9.

36. According to its Notice Letters, on September 7, 2022, Order Express discovered "unusual activity on our computer network."[12]

37. After investigation, Order Express realized that its computer network was openly accessed by an "unknown party" for almost 6 weeks, from July 29, 2022 to September 7, 2022. [13]

38. The Notice Letter does not disclose why the breach was occurring for almost 6 weeks before anyone noticed.[14]

39. By November 18, 2022, according to Order Express's own Notice Letters, it had completed its investigation and was aware of which consumers' PII was affected[15] and that those consumers included Plaintiff(s). Still, Notice Letters were not sent until mid-December 2022.

40. A review of various State Attorneys General websites shows that Order Express only began to notify State Attorney Generals of this Data Breach in mid-December 2022, months after statutory notification was required by the laws of the various states. Time is of the essence when trying to protect against identity theft after a data breach, so early notification is critical.

41. Because of this targeted, intentional cyberattack, data thieves were able to gain access to and obtain data from Order Express that included the Private Information of Plaintiff(s) and Class Members.

42. Order Express admits that the files exfiltrated from Order Express contained at least the following information of Plaintiff(s) and Class Members: name and Social Security number, driver's license or state identification card number, passports, and other information.[16]

---

[12] Notice Letter, Ex. A.
[13] *Id.*
[14] *Id.*
[15] *Id.*
[16] *Data Security Breach Reports*, Tex. Att'y Gen. (Dec. 20, 2022), https://oagtx.force.com/datasecuritybreachreport/apex/DataSecurityReportsPage (last visited Dec. 21, 2022).

43. Upon information and belief, the Private Information stored on Order Express's network was not encrypted.

44. Plaintiff(s)' Private Information was accessed and likely stolen in the Data Breach. Plaintiff(s) reasonably believe their stolen Private Information is currently available for sale on the Dark Web because that is the *modus operandi* of cybercriminals who target businesses that collect highly sensitive Private Information.

45. As a result of the Data Breach, Order Express now encourages Class Members to enroll in credit monitoring, fraud consultation, and identity theft restoration services, a tacit admission of the imminent risk of identity theft faced by Plaintiff(s) and Class Members.[17]

46. That Order Express is encouraging Plaintiff(s) and Class Members to enroll in credit monitoring and identity theft restoration services is an acknowledgment that the impacted consumers are subject to a substantial and imminent threat of fraud and identity theft.

47. Order Express had obligations created by contract, industry standards, and common law to keep Plaintiff(s)'s and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

48. Order Express could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting their equipment and computer files containing PII.

Defendant Acquires, Collects, and Stores PII

49. Order Express acquires, collects, and stores a massive amount of PII of consumers for its business purposes as it provides financial services. Upon information and belief, Order Express may not be properly deleting or destroying the PII records of its former customers.

50. By obtaining, collecting, and using Plaintiff(s)' and Class Members' PII for its own

[17] Notice Letter, Ex. A.

financial gain and business purposes, Defendant assumed legal and equitable duties and knew that it was responsible for protecting Plaintiff(s)' and Class Members' PII from disclosure.

51. Plaintiff(s) and the Class Members have taken reasonable steps to maintain the confidentiality of their PII.

52. Plaintiff(s) and the Class Members relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

The Data Breach was a Foreseeable Risk of which Defendant was on Notice

53. It is well known that PII, including Social Security numbers in particular, is a valuable commodity and a frequent, intentional target of cyber criminals. Companies that collect such information, including Order Express, are well-aware of the risk of being targeted by cybercriminals.

54. Individuals place a high value not only on their PII, but also on the privacy of that data. Identity theft causes severe negative consequences to its victims, as well as severe distress and hours of lost time trying to fight against the impact of identity theft.

55. A data breach increases the risk of becoming a victim of identity theft. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice, "[a] direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the

calculation of out-of-pocket loss."[18]

56. Individuals, like Plaintiff(s) and Class Members, are particularly concerned with protecting the privacy of their Social Security numbers, drivers' license and state identification numbers, and passport information which are the keys to stealing any person's identity and is likened to accessing your DNA for hacker's purposes.

57. In 2021, there were a record 1,862 data breaches last year, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.[19]

58. Additionally in 2021, there was a 15.1% increase in cyberattacks and data breaches since 2020. Over the next two years, in a poll done on security executives, they have predicted an increase in attacks from "social engineering and ransomware" as nation-states and cybercriminals grow more sophisticated. Unfortunately, these preventable causes will largely come from "misconfigurations, human error, poor maintenance, and unknown assets."[20]

59. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, and hopefully can ward off a cyberattack.

60. According to an FBI publication, "[r]ansomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return. Ransomware attacks can cause costly disruptions to operations

---

[18] Erika Harrell, *Victims of Identity Theft, 2018*, U.S. Dep't of Just. (Apr. 2021, NCJ 256085), https://bjs.ojp.gov/content/pub/pdf/vit18.pdf (last visited Dec. 21, 2022).

[19] *Bree Fowler*, *Data breaches break record in 2021*, CNET (Jan. 24, 2022, 12:31 PM), https://www.cnet.com/tech/services-and-software/record-number-of-data-breaches-reported-in-2021-new-report-says/ (last visited Dec. 13, 2022).

[20] Chuck Brooks, *Alarming Cyber Statistics For Mid-Year 2022 That You Need To Know*, Forbes (June 3, 2022, 3:57 PM), https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=176bb6887864 (last visited Dec. 21, 2022).

and the loss of critical information and data." [21] This publication also explains that "[t]he FBI does not support paying a ransom in response to a ransomware attack. Paying a ransom doesn't guarantee you or your organization will get any data back. It also encourages perpetrators to target more victims and offers an incentive for others to get involved in this type of illegal activity." [22]

61. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite its own acknowledgment of its duties to keep PII private and secure, Order Express failed to take appropriate steps to protect the PII of Plaintiff(s) and the proposed Class from being compromised.

At All Relevant Times Order Express Had a Duty to Plaintiff(s) and Class Members to Properly Secure their Private Information

62. At all relevant times, Order Express had a duty to Plaintiff(s) and Class Members to properly secure their PII, encrypt and maintain such information using industry standard methods, train its employees, utilize available technology to defend its systems from invasion, act reasonably to prevent foreseeable harm to Plaintiff(s) and Class Members, and to promptly notify Plaintiff(s) and Class Members when Order Express became aware that their PII was compromised.

63. Order Express had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite its obligation to protect such information. Accordingly, Order Express breached its common law, statutory, and other duties owed to Plaintiff(s) and Class Members.

64. Security standards commonly accepted among businesses that store PII using the

[21] *Ransomware*, FBI, https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware (last visited Dec. 21, 2022).
[22] *Id.*

internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;

c. Monitoring for suspicious or irregular traffic to servers;

d. Monitoring for suspicious credentials used to access servers;

e. Monitoring for suspicious or irregular activity by known users;

f. Monitoring for suspicious or unknown users;

g. Monitoring for suspicious or irregular server requests;

h. Monitoring for server requests for PII;

i. Monitoring for server requests from VPNs; and

j. Monitoring for server requests from Tor exit nodes.

65. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[23] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[24]

66. The ramifications of Order Express's failure to keep consumers' PII secure are long lasting and severe. Once PII is stolen, particularly Social Security and driver's license numbers,

[23] 17 C.F.R. § 248.201 (2013).
[24] *Id*.

fraudulent use of that information and damage to victims including Plaintiff(s) and the Class may continue for years.

The Value of Personal Identifiable Information

67. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200.[25]

68. Criminals can also purchase access to entire company's data breaches from $900 to $4,500.[26]

69. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[27]

70. Attempting to change or cancel a stolen Social Security number is difficult if not

---

[25] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Dec. 21, 2022).

[26] *In the Dark*, VPNOverview (2019), https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/(last visited Dec. 21, 2022).

[27] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed December 21, 2022).

nearly impossible. An individual cannot obtain a new Social Security number without evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

71. Even a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[28]

72. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[29]

73. PII can be used to distinguish, identify, or trace an individual's identity, such as their name and Social Security number. This can be accomplished alone, or in combination with other personal or identifying information that is connected or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.[30]

74. Given the nature of this Data Breach, it is foreseeable that the compromised PII can be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Class Members' PII can easily obtain Class Members' tax returns or open fraudulent

---

[28] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015 4:59 AM), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited Dec. 21, 2022).

[29] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Dec. 21, 2022).

[30] *See* OFFICE OF MGMT. & BUDGET, OMB MEMORANDUM M-07-16 n.1 (last accessed Dec. 21, 2022).

credit card accounts in Class Members' names.

75. The Private Information compromised in this Data Breach is static and difficult, if not impossible, to change (such as Social Security numbers).

76. Moreover, upon information and belief, Order Express has offered either one or two years for identity theft monitoring and identity theft protection through IDX. Its limitation is inadequate when IDX's victims are likely to face many years of identity theft.

77. Furthermore, Defendant Order Express's credit monitoring offer and advice to Plaintiff(s) and Class Members squarely places the burden on Plaintiff(s) and Class Members, rather than on the Defendant, to monitor and report suspicious activities to law enforcement. In other words, Order Express expects Plaintiff(s) and Class Members to protect themselves from its tortious acts resulting in the Data Breach. Rather than automatically enrolling Plaintiff(s) and Class Members in credit monitoring services upon discovery of the breach, Defendant merely sent instructions to Plaintiff(s) and Class Members about actions they can affirmatively take to protect themselves.

78. These services are wholly inadequate as they fail to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud, and they entirely fail to provide any compensation for the unauthorized release and disclosure of Plaintiff(s)' and Class Members' PII.

79. The injuries to Plaintiff(s) and Class Members were directly and proximately caused by Order Express's failure to implement or maintain adequate data security measures for the victims of its Data Breach.

Order Express Failed to Comply with FTC Guidelines

80. Federal and State governments have established security standards and issued

recommendations to mitigate the risk of data breaches and the resulting harm to consumers and financial institutions. The FTC has issued numerous guides for business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[31]

81. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[32] The guidelines note businesses should protect the personal consumer and consumer information that they keep, as well as properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.

82. The FTC emphasizes that early notification to data breach victims reduces injuries: "If you quickly notify people that their personal information has been compromised, they can take steps to reduce the chance that their information will be misused" and "thieves who have stolen names and Social Security numbers can use that information not only to sign up for new accounts in the victim's name, but also to commit tax identity theft. People who are notified early can take steps to limit the damage."[33]

83. The FTC recommends that companies verify that third-party service providers have implemented reasonable security measures.[34]

---

[31] *Start With Security*, FTC (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Dec. 21, 2022).
[32] *Protecting Personal Information: A Guide for Business*, FTC (Oct. 2016), hhttps://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Dec. 21, 2022).
[33] *Data Breach Response*, FTC (Feb. 2021), https://www.ftc.gov/system/files/documents/plain-language/560a_data_breach_response_guide_for_business.pdf (last visited Dec. 1, 2022).
[34] *Start With Security*, FTC, *supra* note 31.

84. The FTC recommends that businesses:

a. Identify all connections to the computers where you store sensitive information.

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks.

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to

allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

85. The FTC has brought enforcement actions against businesses for failing to protect consumer and consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

86. Because Class Members entrusted Order Express with their PII, Order Express had, and has, a duty to the Plaintiff(s) and Class Members to keep their PII secure.

87. Plaintiff(s) and the other Class Members reasonably expected that when they provide PII to Order Express, it would safeguard their PII.

88. Order Express was at all times fully aware of its obligation to protect the personal and financial data of consumers, including Plaintiff(s) and members of the Class. Order Express was also aware of the significant repercussions if it failed to do so. Its own Privacy Policy and

Notice Letter, quoted above, acknowledges this awareness.

89. Order Express's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—including Plaintiff(s)' and Class Members' first names, last names, addresses, and Social Security numbers, and other highly sensitive and confidential information—constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Plaintiff(s) and Class Members Have Suffered Concrete Injuries.

90. Plaintiff(s) and Class Members reasonably expected that Defendant would provide adequate security protections for their PII, and Class Members provided Defendant with sensitive personal information, including their names, addresses, and Social Security numbers.

91. Defendant's poor data security deprived Plaintiff(s) and Class Members of the benefit of their bargain. Plaintiff(s) and other individuals whose PII was entrusted with Order Express understood and expected that, as part of that business relationship, they would receive data security, when in fact Defendant did not provide the expected data security. Accordingly, Plaintiff(s) and Class Members received data security that was of a lesser value than what they reasonably expected. As such, Plaintiff(s) and the Class Members suffered pecuniary injury.

92. Cybercriminals intentionally attack and exfiltrate PII to exploit it. Thus, Class Members are now, and for the rest of their lives will be, at a heightened and substantial risk of identity theft. Plaintiff(s) have also incurred (and will continue to incur) damages in the form of, inter alia, loss of privacy and costs of engaging adequate credit monitoring and identity theft protection services.

93. The cybercriminals who obtained the Class Members' PII may exploit the information they obtained by selling the data in so-called "dark markets" or on the "dark web."

Having obtained these names, addresses, Social Security numbers, and other PII, cybercriminals can pair the data with other available information to commit a broad range of fraud in a Class Member's name, including but not limited to:

- obtaining employment;
- obtaining a loan;
- applying for credit cards or spending money;
- filing false tax returns;
- stealing Social Security and other government benefits; and
- applying for a driver's license, birth certificate, or other public document.

94. In addition, if a Class Member's Social Security number is used to create false identification for someone who commits a crime, the Class Member may become entangled in the criminal justice system, impairing the person's ability to gain employment or obtain a loan.

95. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Data Breach, Plaintiff(s) and the other Class Members have been deprived of the value of their PII, for which there is a well-established national and international market.

96. Furthermore, PII has a long shelf-life because it contains different forms of personal information, it can be used in more ways than one, and it typically takes time for an information breach to be detected.

97. Accordingly, Defendant's wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiff(s) and the other Class Members at an imminent, immediate, and continuing increased risk of identity theft and identity fraud. Indeed, "[t]he level of risk is growing for anyone whose information is stolen in a data breach." Javelin Strategy & Research, a leading provider of quantitative and qualitative research, notes that "[t]he theft of SSNs places consumers

at a substantial risk of fraud."[35] Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that have not yet been exploited by cybercriminals bears a high risk that the cybercriminals who now possess Class Members' PII will do so at a later date or re-sell it.

98. As a result of the Data Breach, Plaintiff(s) and Class Members have already suffered injuries, and each are at risk of a substantial and imminent risk of future identity theft.

Plaintiff Dillard's Experience

99. Plaintiff Porscha Dillard is, and at all times relevant to this Complaint was, a resident and citizen of the State of California.

100. Plaintiff Dillard is a consumer who was apparently affiliated service provided by Order Express. Upon information and belief, Order Express may have required that a customer to provide it with her PII, or possibly she received a payment for which she was required to provide PII. She is unsure of how Order Express received her PII.

101. On or about December 19, 2022, Plaintiff Dillard received the Notice of Data Breach letter, which indicated that Order Express had known about the Data Breach for months. The letter informed her that her PII was accessed by an "unknown party." The letter stated that the impacted information may have included her name and her driver's license number, but did not expand on whether additional information was stolen as well.

102. Plaintiff Dillard is alarmed by her Personal Information being accessed and stolen by an unknown cybercriminal, and even more by the fact that her PII was identified as among the

[35] Al Pascual, *The Consumer Data Insecurity Report: Examining The Data Breach- Identity Fraud Paradigm In Four Major Metropolitan Areas*, Nat'l Consumers League (June 2014), https://www.it.northwestern.edu/bin/docs/TheConsumerDataInsecurityReport_byNCL.pdf (last visited Dec. 21, 2022).

breach data on Order Express's computer system despite not being completely aware of her relationship to this company.

103. Plaintiff Dillard has been receiving a combination of around 3 spam calls and many spam emails per day. She believes that the increased spam she is receiving is related to this Data Breach.

104. Plaintiff Dillard is concerned that the spam calls and texts are being placed with the intent of obtaining more personal information from her and committing identity theft by way of a social engineering attack.

105. In response to Order Express's Notice of Data Breach, Plaintiff will be required to spend time dealing with the consequences of the Data Breach, which will continue to include time spent verifying the legitimacy of the Notice of Data Breach, exploring credit monitoring and identity theft insurance options, self-monitoring her accounts, and freezing her credit. She realizes she will likely have to spend about an hour a day verifying financial accounts to check for fraudulent activities. The time she is forced to spend monitoring and securing her accounts has been lost forever and cannot be recaptured.

106. Immediately after receiving the Notice Letter, Plaintiff spent time discussing her options with a law firm, froze her credit, and had to get a new driver's license in an effort to mitigate the damage caused by Order Express.

107. Plaintiff is very careful about sharing PII and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

108. Plaintiff suffered actual injury in the form of damages and diminution in the value of her PII—a form of intangible property that she entrusted to Order Express (or its customer).

109. Plaintiff has suffered lost time, annoyance, interference, and inconvenience as a

result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

110. Plaintiff Dillard reasonably believes that her Private Information may have already been sold by the cybercriminals. Had she been notified of Order Express's breach in a timelier manner, she could have attempted to mitigate her injuries.

111. Plaintiff Dillard has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her stolen PII being placed in the hands of unauthorized third parties and possibly criminals.

112. Plaintiff has a continuing interest in ensuring that her PII, which upon information and belief remains backed up and in Order Express's possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

113. Plaintiff(s) bring this action on behalf of themselves and on behalf of all other persons similarly situated ("the Class") under Federal Rule of Civil Procedure 23.

114. Plaintiff(s) propose the following Class definition, subject to amendment as appropriate:

> All persons whose Private Information was maintained on Defendant Order Express, Inc.'s computer systems and compromised in its Data Breach that occurred between July and September 2022.

115. Plaintiff(s) propose the following California Subclass definition, subject to amendment as appropriate:

> All persons who reside in California and whose Private Information was maintained on Defendant Order Express, Inc.'s computer systems and compromised in its Data Breach that occurred between July and September 2022.

116. Excluded from the Class are Defendant's officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys,

successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

117. Plaintiff(s) hereby reserves the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

118. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff(s) at this time, based on Defendant's reports to State Attorney Generals, the Class consists of approximately 63,220 persons whose data was compromised in Data Breach.

119. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff(s)' and Class Members' Private Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendant breached its duty to Class Members to safeguard their

Private Information;

g. Whether computer hackers obtained Class Members' Private Information in the Data Breach;

h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Plaintiff(s) and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

l. Whether Defendant's acts, inactions, and practices complained of herein violated the California statutes invoked below;

m. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and

n. Whether Plaintiff(s) and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

120. Typicality. Plaintiff(s)' claims are typical of those of other Class Members because Plaintiff(s)'s Private Information, like that of every other Class Member, was compromised in the Data Breach.

121. Adequacy of Representation. Plaintiff(s) will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff(s)' Counsel are competent and experienced in litigating class actions.

122. Predominance. Defendant has engaged in a common course of conduct toward

Plaintiff(s) and Class Members, in that all the Plaintiff(s)' and Class Members' Private Information was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

123. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

124. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

125. Likewise, particular issues under Fed. R. Civ. P. 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff(s) and the Class to exercise

due care in collecting, storing, and safeguarding their Private Information;

b. Whether Defendant's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;

c. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

d. Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and

e. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

126. Finally, all Members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Upon information and belief, Class Members have already been preliminarily identified and sent notice of the Data Breach by Order Express.

CAUSES OF ACTION

FIRST COUNT
Negligence
(On behalf of Plaintiff(s) and All Class Members)

127. Plaintiff(s) re-allege and incorporate by reference the paragraphs above as if fully set forth herein.

128. Order Express owed a duty to Plaintiff(s) and Class Members to exercise reasonable care in safeguarding and protecting their PII in its possession, custody, or control.

129. Plaintiff(s) and the Class Members entrusted their PII to Defendant with the understanding that Defendant would safeguard their information.

130. Order Express had full knowledge of the sensitivity of the PII and the types of harm

that Plaintiff(s) and Class Members could and would suffer if the PII were wrongfully disclosed.

131. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer network—and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

132. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

133. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII.

134. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. Failing to adequately monitor the security of its networks and systems;

c. Failing to periodically ensure that its email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' PII;

e. Failing to detect in a timely manner that Class Members' PII had been compromised; and

f. Failing to promptly notify Class Members of the breach so they might mitigate their damages and protect their Private Information.

135. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the industry.

136. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII would result in one or more types of injuries to Class Members.

137. There is a temporal and close causal connection between Defendant's failure to implement security measures to protect the PII and the harm suffered, and an imminent and substantial risk of harm that will be suffered by Plaintiff(s) and the Class.

138. As a result of Defendant's negligence, Plaintiff(s) and the Class Members have suffered and will continue to suffer damages and injury including, but not limited to: out-of-pocket expenses associated with procuring robust identity protection and restoration services; increased risk of future identity theft and fraud, the costs associated therewith; time spent monitoring, addressing and correcting the current and future consequences of the Data Breach; and the necessity to engage legal counsel and incur attorneys' fees, costs and expenses.

139. Plaintiff(s) and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

140. Plaintiff(s) and Class Members are also entitled to injunctive relief requiring

Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

SECOND COUNT
Negligence *Per Se*
(On Behalf of Plaintiff(s) and All Class Members)

141. Plaintiff(s) re-allege and incorporate by reference the paragraphs above as if fully set forth herein.

142. Section 5 of the FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant's, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

143. Order Express violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of the Data Breach for companies of its type, including, specifically, the immense damages that would result to Plaintiff(s) and Members of the Class due to the valuable nature of the PII at issue in this case—including Social Security numbers.

144. Defendants' violations of Section 5 of the FTCA constitute negligence per se.

145. Plaintiff(s) and Members of the Class are within the class of persons that the FTCA was intended to protect.

146. The harm that occurred as a result of the Data Breach is the type of harm the FTCA was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and

deceptive practices, caused the same harm as that suffered by Plaintiff(s) and Members of the Class.

147. As a direct and proximate result of Defendant's negligence per se, Plaintiff(s) and Members of the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII of customers in its continued possession; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff(s) and Members of the Class.

148. Additionally, as a direct and proximate result of Defendants' negligence per se, Plaintiff(s) and Members of the Class have suffered and will suffer the continued risks of exposure of their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in their continued possession.

149. Plaintiff(s)' and Class Members' Private Information constitutes personal property

that was stolen due to Order Express's negligence, resulting in harm, injury and damages to Plaintiff(s) and Class Members.

150. Order Express's conduct in violation of applicable laws directly and proximately caused the unauthorized access and disclosure of Plaintiff(s)' and Class Members' unencrypted Private Information.

151. Plaintiff(s) and Class Members have suffered and will continue to suffer damages as a result of Order Express's conduct. Plaintiff(s) and Class Members seek damages and other relief as a result of Order Express's negligence.

THIRD COUNT
Breach of Implied Contract
(On Behalf of Plaintiff(s) and All Class Members)

152. Plaintiff(s) re-allege and incorporate by reference the paragraphs above as if fully set forth herein.

153. Plaintiff(s) and Class Members were required to provide their PII to Defendant as a condition of receiving services provided by Defendant.

154. Plaintiff(s) and Class Members provided their PII to Defendant or its third-party agents in exchange for Order Express's services or employment. In exchange for the PII, Defendant promised to protect their PII from unauthorized disclosure.

155. At all relevant times Defendant promulgated, adopted, and implemented written a Privacy Policy whereby it expressly promised Plaintiff(s) and Class Members that it would only disclose PII under certain circumstances, none of which relate to the Data Breach.

156. On information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiff(s)' and Class Members' PII would remain protected.

157. Implicit in the agreement between Plaintiff(s) and Class Members and the

Defendant to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiff(s) and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiff(s) and Class Members from unauthorized disclosure or uses, (f) retain the PII only under conditions that kept such information secure and confidential.

158. When Plaintiff(s) and Class Members provided their PII to Defendant as a condition of relationship, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

159. Defendant required Class Members to provide their PII as part of Defendant's regular business practices.

160. In entering into such implied contracts, Plaintiff(s) and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

161. Plaintiff(s) and Class Members would not have entrusted their PII to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure. Plaintiff(s) and Class Members would not have entrusted their PII to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

162. Plaintiff(s) and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

163. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their PII.

164. As a direct and proximate result of Defendant's breaches of the implied contracts, Class Members sustained damages as alleged herein.

165. Plaintiff(s) and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

166. Plaintiff(s) and Class Members are also entitled to nominal damages for the breach of implied contract.

167. Plaintiff(s) and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate long term credit monitoring to all Class Members for a period longer than the grossly inadequate one-year currently offered.

FOURTH COUNT
Breach of Fiduciary Duty
(On Behalf of Plaintiff(s) and Class Members)

168. Plaintiff(s) re-allege the above allegations as if fully set forth herein.

169. In light of the special relationship between Defendant Order Express and Plaintiff(s) and Class Members, whereby Defendant became guardian of Plaintiff(s)' and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for Plaintiff(s) and Class Members, (1) for the safeguarding of Plaintiff(s)' and Class Members' Private Information; (2) to timely notify Plaintiff(s) and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

170. Defendant has a fiduciary duty to act for the benefit of Plaintiff(s) and Class Members upon matters within the scope of Order Express's relationship with its customers and

former customers, in particular, to keep secure their Private Information.

171. Defendant breached its fiduciary duties to Plaintiff(s) and Class Members by failing to diligently discovery, investigate, and give notice of the Data Breach in a reasonable and practicable period of time.

172. Defendant breached its fiduciary duties to Plaintiff(s) and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff(s)' and Class Members' Private Information.

173. Defendant breached its fiduciary duties owed to Plaintiff(s) and Class Members by failing to timely notify and/or warn Plaintiff(s) and Class Members of the Data Breach.

174. Defendant breached its fiduciary duties to Plaintiff(s) and Class Members by otherwise failing to safeguard Plaintiff(s)' and Class Members' Private Information.

175. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff(s) and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in their continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of

the lives of Plaintiff(s) and Class Members; and (vii) the diminished value of Defendant's services they received.

176. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff(s) and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

FIFTH COUNT
Intrusion Upon Seclusion / Invasion of Privacy
(On Behalf of Plaintiff(s) and All Class Members)

177. Plaintiff(s) re-allege the above allegations as if fully set forth herein.

178. The State of California recognizes the tort of Intrusion upon Seclusion, and adopts the formulation of that tort found in the Restatement (Second) of Torts, which states:

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

Restatement (Second) of Torts § 652B (1977).

179. Plaintiff(s) and Class Members had a reasonable expectation of privacy in the Private Information Defendant mishandled.

180. Defendant's conduct as alleged above intruded upon Plaintiff(s)' and Class Members' seclusion under common law.

181. By intentionally failing to keep Plaintiff(s)' and Class Members' Private Information safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant intentionally invaded Plaintiff(s)' and Class Members' privacy by:

a. Intentionally and substantially intruding into Plaintiff(s)' and Class Members' private affairs in a manner that identifies Plaintiff(s) and Class Members and

that would be highly offensive and objectionable to an ordinary person; and

b. Intentionally publicizing private facts about Plaintiff(s) and Class Members, which is highly offensive and objectionable to an ordinary person; and

c. Intentionally causing anguish or suffering to Plaintiff(s) and Class Members.

182. Defendant knew that an ordinary person in Plaintiff(s)' or Class Members' position would consider Defendant's intentional actions highly offensive and objectionable.

183. Defendant invaded Plaintiff(s)' and Class Members' right to privacy and intruded into Plaintiff(s)' and Class Members' private affairs by intentionally misusing and/or disclosing their Private Information without their informed, voluntary, affirmative, and clear consent.

184. Defendant intentionally concealed from and delayed reporting to Plaintiff(s) and Class Members a security incident that misused and/or disclosed their Private Information without their informed, voluntary, affirmative, and clear consent.

185. The conduct described above was at or directed at Plaintiff(s) and the Class Members.

186. As a proximate result of such intentional misuse and disclosures, Plaintiff(s)' and Class Members' reasonable expectations of privacy in their Private Information was unduly frustrated and thwarted. Defendant's conduct amounted to a substantial and serious invasion of Plaintiff(s)' and Class Members' protected privacy interests causing anguish and suffering such that an ordinary person would consider Defendant's intentional actions or inaction highly offensive and objectionable.

187. In failing to protect Plaintiff(s)' and Class Members' Private Information, and in intentionally misusing and/or disclosing their Private Information, Defendant acted with intentional malice and oppression and in conscious disregard of Plaintiff(s)' and Class Members'

rights to have such information kept confidential and private. Plaintiff(s), therefore, seek an award of damages on behalf of themselves and the Class.

SIXTH COUNT
Unjust Enrichment
(On Behalf of Plaintiff(s) and All Class Members)

188. Plaintiff(s) re-allege and incorporate by reference the paragraphs above as if fully set forth herein.

189. Plaintiff(s) and Class Members conferred a monetary benefit on Defendant in the form of the provision of their PII and Defendant would be unable to engage in its regular course of business without that PII.

190. Defendant appreciated that a monetary benefit was being conferred upon it by Plaintiff(s) and Class Members and accepted that monetary benefit.

191. However, acceptance of the benefit under the facts and circumstances outlined above make it inequitable for Defendant to retain that benefit without payment of the value thereof. Specifically, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff(s)' and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiff(s) and Class Members by utilizing cheaper, ineffective security measures. Plaintiff(s) and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite data security.

192. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary benefit belonging to Plaintiff(s) and Class Members, because Defendant failed to implement appropriate data management and security measures.

193. Defendant acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

194. If Plaintiff(s) and Class Members had known that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

195. Plaintiff(s) and Class Members have no adequate remedy at law.

196. As a direct and proximate result of Defendant's conduct, Plaintiff(s) and Class Members have suffered or will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff(s) and Class Members.

197. As a direct and proximate result of Defendant's conduct, Plaintiff(s) and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

198. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff(s) and Class Members, proceeds that they unjustly received from them.

SEVENTH COUNT
Declaratory Judgment
(On Behalf of Plaintiff(s) and All Class Members)

199. Plaintiff(s) re-allege and incorporate by reference the paragraphs above as if fully set forth herein.

200. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

201. An actual controversy has arisen in the wake of the Order Express data breach regarding its present and prospective common law and other duties to reasonably safeguard its customers' Private Information and whether Order Express is currently maintaining data security measures adequate to protect Plaintiff(s) and Class Members from further data breaches that compromise their Private Information.

202. Plaintiff(s) allege that Order Express' data security measures remain inadequate. Plaintiff(s) will continue to suffer injury because of the compromise of their Private Information and remain at imminent risk that further compromises of their Private Information will occur in the future.

203. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Order Express continues to owe a legal duty to secure consumers' Private Information and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and various states' statutes; and

b. Order Express continues to breach this legal duty by failing to employ

reasonable measures to secure consumers' Private Information.

204. The Court also should issue corresponding prospective injunctive relief requiring Order Express to employ adequate security protocols consistent with law and industry standards to protect consumers' Private Information.

205. If an injunction is not issued, Plaintiff(s) and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Order Express. The risk of another such breach is real, immediate, and substantial. If another breach at Order Express occurs, Plaintiff(s) and class members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

206. The hardship to Plaintiff(s) and Class Members if an injunction does not issue exceeds the hardship to Order Express if an injunction is issued. Among other things, if another data breach occurs at Order Express, Plaintiff(s) and Class Members will likely be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Order Express of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Order Express has a pre-existing legal obligation to employ such measures.

207. Issuance of the requested injunction will not do a disservice to the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Order Express, thus eliminating the additional injuries that would result to Plaintiff(s) and thousands of consumers whose Private Information would be further compromised.

EIGHTH COUNT
Violation of the California Unfair Competition Law,
Cal. Bus. & Prof Code §§ 17200, *et seq.* – Unlawful Business Practices
(On Behalf of Plaintiff(s) and California Subclass Members)

208. Plaintiff(s) restate and reallege the foregoing paragraphs as if fully set forth herein.

Plaintiff(s) brings this claim on behalf of herself and California Subclass Members ("Class" for the purposes of this claim).

209. Defendant violated Cal. Bus. and Prof. Code §§ 17200, *et seq.*, by engaging in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in Cal. Bus. Prof. Code § 17200 with respect to the services provided to the Class.

210. Defendant engaged in unlawful acts and practices with respect to the services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiff(s)' and Class Members' Private Information with knowledge that the information would not be adequately protected; and by storing Plaintiff(s)' and Class Members' Private Information in an unsecure electronic environment in violation of California's data breach statute, Cal. Civ. Code § 1798.81.5, which requires Defendants to take reasonable methods of safeguarding the Private Information of Plaintiff(s) and the Class Members.

211. In addition, Defendant engaged in unlawful acts and practices by failing to disclose the Data Breach in a timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code § 1798.82.

212. As a direct and proximate result of Defendant's unlawful practices and acts, Plaintiff(s) and Class Members were injured and lost money or property, including but not limited to the price received by Defendants for the services, the loss of Plaintiff(s)' and Class Members' legally protected interest in the confidentiality and privacy of their Private Information, nominal damages, and additional losses as described herein.

213. Defendant knew or should have known that Defendant's computer systems and data security practices were inadequate to safeguard Plaintiff(s)' and Class Members' Private

Information and that the risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff(s) and Class Members.

214. Plaintiff(s), on behalf of the Class, seek relief under Cal. Bus. & Prof. Code §§ 17200, *et seq.*, including, but not limited to, restitution to Plaintiff(s) and Class Members of money or property that Defendant may have acquired by means of Defendant's unlawful, and unfair business practices, restitutionary disgorgement of all profits accruing to Defendant because of Defendant's unlawful and unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

215. Plaintiff(s), on behalf of the Class, seek relief under Cal. Bus. & Prof. Code § 17200, et seq., including, but not limited to, restitution to Plaintiff(s) and Class Members of money or property that Defendants may have acquired by means of Defendants' unlawful, and unfair business practices, restitutionary disgorgement of all profits accruing to Defendants because of Defendants' unlawful and unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

NINTH COUNT
Violation of California Consumers Legal Remedies Act,
Cal. Civ. Code §§ 1750, *et seq.*
(On Behalf of Plaintiff(s) and California Subclass Members)

216. Plaintiff(s) restate and reallege the foregoing paragraphs as if fully set forth herein. Plaintiff(s) brings this claim on behalf of herself and California Subclass Members ("Class" for the purposes of this claim).

217. This cause of action is brought pursuant to the California Consumers Legal Remedies Act (the "CLRA"), Cal. Civ. Code §§ 1750, *et seq.*

218. Defendant is the party with the most knowledge of the underlying facts giving rise to Plaintiff(s)' allegations, so that any pre-suit notice would not put Defendant in a better position

to evaluate those claims. To the extent additional notice is required, Plaintiff(s) will issue separate demands under Cal. Civ. Code § 1782(a).

219. Plaintiff(s) and Class Members are "consumers," as the term is defined by Cal. Civ. Code § 1761(d).

220. Plaintiff(s), Class Members, and Defendant have engaged in "transactions," as that term is defined by Cal. Civ. Code § 1761(e).

221. The conduct alleged in this Complaint constitutes unfair methods of competition and unfair and deceptive acts and practices for the purpose of the CLRA, and the conduct was undertaken by Defendant was likely to deceive consumers.

222. Cal. Civ. Code § 1770(a)(5) prohibits one who is involved in a transaction from "[r]epresenting that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have."

223. Defendant violated this provision by representing that it took appropriate measures to protect Plaintiff(s)' and the Class Members' Private Information. Additionally, Defendant improperly handled, stored, or protected either unencrypted or partially encrypted data.

224. As a result, Plaintiff(s) and Class Members were induced to enter into a relationship with Defendant and provide their Private Information.

225. As a result of engaging in such conduct, Defendant has violated Cal. Civ. Code § 1770.

226. Pursuant to Civil Code § 1780(a)(2) and (a)(5), Plaintiff(s) seek an order of this Court that includes, but is not limited to, an order enjoining Defendant from continuing to engage in unlawful, unfair, or fraudulent business practices or any other act prohibited by law.

227. Plaintiff(s) and Class Members suffered injuries caused by Defendant's

misrepresentations, because they provided their Private Information believing that Defendant would adequately protect this information.

228. Plaintiff(s) and Class Members may be irreparably harmed and/or denied an effective and complete remedy if such an order is not granted.

229. The unfair and deceptive acts and practices of Defendant, as described above, present a serious threat to Plaintiff(s) and Class Members.

TENTH COUNT
Violation of California Consumer Records Act,
Cal. Civ. Code §§ 1798.80, *et seq.*
(On Behalf of Plaintiff(s) and California Subclass Members)

230. Plaintiff(s) restate and reallege the foregoing paragraphs as if fully set forth herein. Plaintiff(s) brings this claim on behalf of herself and California Subclass Members ("Class" for the purposes of this claim).

231. Section 1798.2 of the California Civil Code requires any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" to "disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Under section 1798.82, the disclosure "shall be made in the most expedient time possible and without unreasonable delay . . .."

232. The CCRA further provides: "Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82(b).

233. Any person or business that is required to issue a security breach notification under the CCRA shall meet all of the following requirements:

a. The security breach notification shall be written in plain language;

b. The security breach notification shall include, at a minimum, the following information:

i. The name and contact information of the reporting person or business subject to this section;

ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;

iii. If the information is possible to determine at the time the notice is provided, then any of the following:

1. The date of the breach;

2. The estimated date of the breach; or

3. The date range within which the breach occurred. The notification shall also include the date of the notice.

iv. Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided;

v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided; and

vi. The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a Social Security number or a driver's license or California identification card number.

234. The Data Breach described herein constituted a "breach of the security system" of Defendant.

235. As alleged above, Defendant unreasonably delayed informing Plaintiff(s) and Class Members about the Data Breach, affecting their Personal Information for approximately 4 months after Defendant knew the Data Breach had occurred.

236. Defendant failed to disclose to Plaintiff(s) and Class Members, without unreasonable delay and in the most expedient time possible, the breach of security of their unencrypted, or not properly and securely encrypted, Personal Information when Defendant knew or reasonably believed such information had been compromised.

237. Defendant's ongoing business interests gave Defendant incentive to conceal the Data Breach from the public to ensure continued revenue.

238. Upon information and belief, no law enforcement agency instructed Defendant that timely notification to Plaintiff(s) and Class Members would impede its investigation.

239. As a result of Defendant's violation of Cal. Civ. Code § 1798.82, Plaintiff(s) and Class Members were deprived of prompt notice of the Data Breach and were thus prevented from taking appropriate protective measures, such as securing identity theft protection or requesting a credit freeze. These measures could have prevented some of the damages suffered by Plaintiff(s) and Class Members because their stolen information would have had less value to identity thieves.

240. As a result of Defendant's violation of Cal. Civ. Code § 1798.82, Plaintiff(s) and Class Members suffered incrementally increased damages separate and distinct from those simply caused by the Data Breach itself.

241. Plaintiff(s) and Class Members seek all remedies available under Cal. Civ. Code § 1798.84, including, but not limited to the damages suffered by Plaintiff(s) and Class Members as

alleged above and equitable relief.

242. Defendant's misconduct as alleged herein is fraud under Cal. Civ. Code § 3294(c)(3) in that it was deceit or concealment of a material fact known to the Defendant conducted with the intent on the part of Defendant of depriving Plaintiff(s) and Class Members of "legal rights or otherwise causing injury." In addition, Defendant's misconduct as alleged herein is malice or oppression under Cal. Civ. Code § 3294(c)(1) and (c)(2) in that it was despicable conduct carried on by Defendant with a willful and conscious disregard of the rights or safety of Plaintiff(s) and Class Members and despicable conduct that has subjected Plaintiff(s) and Class Members to hardship in conscious disregard of their rights. As a result, Plaintiff(s) and Class Members are entitled to punitive damages against Defendants under Cal. Civ. Code § 3294(a).

243. Defendants' misconduct as alleged herein is fraud under Cal. Civ. Code § 3294(c)(3) in that it was deceit or concealment of a material fact known to the Defendant conducted with the intent on the part of Defendant of depriving Plaintiff(s) and Class Members of "legal rights or otherwise causing injury." In addition, Defendant's misconduct as alleged herein is malice or oppression under Cal. Civ. Code § 3294(c)(1) and (c)(2) in that it was despicable conduct carried on by Defendant with a willful and conscious disregard of the rights or safety of Plaintiff(s) and Class Members and despicable conduct that has subjected Plaintiff(s) and Class Members to hardship in conscious disregard of their rights. As a result, Plaintiff(s) and Class Members are entitled to punitive damages against Defendants under Cal. Civ. Code § 3294(a).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff(s) pray for judgment as follows:

A. For an Order certifying this action as a class action and appointing Plaintiff(s) and their counsel to represent the Class and the California Subclass;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff(s)' and Class

Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures of its Data Breach to Plaintiff(s) and Class Members;

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

E. For declaratory relief as requested;

F. Ordering Defendant to pay for lifetime credit monitoring services for Plaintiff(s) and the Class;

G. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

H. For an award of punitive damages, as allowable by law;

I. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

J. Pre- and post-judgment interest on any amounts awarded; and

K. Such other and further relief as this Court may deem just and proper.

DATED this 22nd day of December 2022.

Respectfully submitted,

By: /s/*Gary E. Mason*
Gary E. Mason
Danielle L. Perry
Lisa A. White*
MASON LLP
5101 Wisconsin Ave. NW, Suite 305
Washington, DC 20016

Telephone: 202.429.2290
gmason@masonllp.com
dperry@masonllp.com
lwhite@masonllp.com
Attorneys for Plaintiff(s) and the proposed Class

Theodore B. Bell (IL Bar No. 6273743)
MASON LLP
8045 Kenneth Ave.
Skokie, IL 60076
Telephone: 202.640.1169
tbell@masonllp.com

Local Counsel for Plaintiff(s) and the proposed Class

**pro hac vice applications for admission to be filed.*